FORM PTO-1390
(REV 11-2000)

U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. § 371

ATTORNEY'S DOCKET NUMBER
449122008300

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
Not yet assigned 09/890913

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE00/00284	**01 February 2000**	**08 February 1999**

TITLE OF INVENTION
ARRANGEMENT FOR CAPTURING AND EVALUATING DATA OR SIGNALS, AND METHOD FOR CHECKING THE IDENTITY OR AUTHORIZATION OF A PERSON

APPLICANT(S) FOR DO/EO/US
Manfred BROMBA

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is attached hereto (required only if not communicated by the International Bureau).
   b. ☐ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application under PCT Article 19 (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)).
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A substitute specification.
16 ☐ A change of power of attorney and/or address letter.
17 ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18 ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
19 ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. ☒ Other items or information: 1) IPER; 2) Int'l Search Report; 3) Application Data Sheet 4) Return receipt postcard.

CERTIFICATE OF HAND DELIVERY

I hereby certify that this correspondence is being hand filed with the United States Patent and Trademark Office in Washington, D.C. on August 8, 2001.

R. Lynn Boyden

R. Lynn Boyden

U.S. APPLICATION NO. (if known, see 37 CFR 1.5) Not yet assigned 09/890913	INTERNATIONAL APPLICATION NO. PCT/DE00/00284	ATTORNEY'SDOCKET NUMBER 449122008300

21. ☒ The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(5)):

CALCULATIONS
PTO USE ONLY

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO..........................$1,000.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO......................$860.00

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO..........................$710.00

International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provision of PCT Article 33(1)-(4) $690.00

International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) $100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =				$860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).				$0	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	10 - 20 =	0	x $18.00	$0	
Independent claims	2 - 3 =	0	x $80.00	$0	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $270.00	$270.00	
TOTAL OF ABOVE CALCULATIONS =				$1,130	
□ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by ½.				$0	
SUBTOTAL =				$1,130	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$0	
TOTAL NATIONAL FEE =				$1,130	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00 per property** +				$40.00	
TOTAL FEES ENCLOSED =				$1,170	
				Amount to be refunded:	$
				charged:	$

a. ☒ Please charge my **<u>Deposit Account No. 03-1952</u>** in the amount of $1,170.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

b. ☒ The Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment to **<u>Deposit Account No. 03-1952</u>**. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Kevin R. Spivak
Morrison & Foerster LLP
2000 Pennsylvania Avenue, N.W.
Washington, D.C. 20006-1888

Kevin R Spivak
SIGNATURE

Kevin R. Spivak
Registration No. 43,148

Description

Arrangement for capturing and evaluating data or signals, and method for checking the identity or authorization of a person

In connection with the increasing spread of information technology systems, methods for checking the identity or authorization of persons are quickly becoming more important. A common feature of all known methods of this type is that an authorized person identifies himself to an information technology system using an item of information or a feature which is known only to this person or which is characteristic of this person, is unique and is unalterable.

Biometric features, such as fingerprint patterns, iris patterns and similar characteristic properties of a person are distinguished by their uniqueness and unalterability. This means that any person can easily be identified by such biometric features using information technology systems. A secret password is also a characteristic feature of a person, so long as the password has not been given away. Biometric features and passwords are therefore well suited, in principle, to the aforementioned purposes.

Modern biometric verification methods detect the biometric features of a person using a special sensor, initially in the form of raw data. Special algorithms can be used to extract the actual features from these raw data. Verification or identification then takes place by comparing a stored set of reference features with the current features.

It is evident that the security of the method is essentially dependent on the raw data, the extracted sets of features or the passwords not getting into the hands of unauthorized parties. In systems which are known today, this requirement is not satisfied or is satisfied only insufficiently, however. The invention is based on the object of improving this situation. This object is achieved using an arrangement for capturing and evaluating data or signals having features in accordance with claim 1 and by a method for checking the identity or authorization of a person having features in accordance with claim 5.

In this context, the invention is based on the idea of not transferring a person's characteristic data to a foreign system, but rather of capturing these data or signals using an arrangement carried by the authorized person, and using this arrangement to encrypt input data obtained by the arrangement from a foreign system, so that the foreign system does not identify authorization of the person by his features, which need to be protected, of course, but rather by the correct encryption of the input data. In this case, the whole process of feature identification and of input data encryption takes place within the arrangement, which is preferably particularly protected against unauthorized access. This effectively protects a person's characteristic data from misuse.

Advantageous developments of the invention are the subject matter of subclaims.

The invention is described below using preferred exemplary embodiments and with reference to a figure.

Figure 1 shows, schematically, the design of a preferred embodiment of the invention, and at the same time clarifies the course of an inventive method.

An inventive arrangement for capturing and evaluating data or signals, in particular for checking the identity or authorization of a person, etc., comprises a device (DE) for capturing data (D) or signals (S), a device (DV) for checking the captured data or signals within the arrangement, and a device (KE) for encrypting input data (ED) within the arrangement.

The device for capturing data or signals may be a simple keyboard of a computer or communication terminal or of another small appliance. Of course, instead of a keyboard, it is also possible to use a graphical input medium, such as a pressure-sensitive input surface, perhaps with a display located underneath. Such input devices are particularly suitable for capturing passwords or signatures.

The device for capturing data or signals may alternatively be a microphone, or a camera, or a fingerprint sensor. Further devices, in particular for detecting biometric features of a person, are conceivable. The captured data or signals may comprise anything from text, numerals, handwriting, words or sentences spoken through voice tests which is suitable for identification or for checking the authorization of a person. These data or signals are checked directly, or after extraction of feature data (MD), by a checking device (DV). In accordance with the present invention, this checking device is located within the arrangement. The data or signals to be checked or the feature data extracted therefrom therefore do not leave the arrangement for checking purposes.

The user can therefore, at least as long as he remains the sole proprietor of the arrangement and can exclude intervention by unauthorized parties, be sure that his data cannot be misused. If the check is carried out successfully (positively), i.e. the captured data and signals indicate, for the purposes of the check, input by an authorized user, the input data (ED) supplied to the arrangement from the outside are encrypted within the arrangement using a device (KE) for encryption.

An external system can now check correct encryption of the input data, and hence the identity of the person or his authorization, at any time. To this end, it is merely necessary to read and check the encrypted input data. The person's characteristic data remain in the arrangement and are therefore protected from misuse.

The personal data can be checked within the arrangement in a wide variety of different ways. First, it is possible for the key which is needed for encrypting the input data to be calculated directly from the captured data or signals or from the feature data extracted therefrom. Another option is for the feature data to be supplied to a decision function which directly ascertains the result of the check in the form of a yes/no decision. Simplest of all, by contrast, is probably direct comparison of the data, signals or feature data with reference data (RD) stored in a memory device (SE1) in the arrangement. However, the two aforementioned methods have the advantage that the data to be protected are themselves not stored in the arrangement, and are thus better protected from misuse.

If the key (K) is not calculated directly within the arrangement, it is advantageous for it to be stored in a memory device (SE2) within the arrangement. Another option would be to use a "hardwired" algorithm for encryption, in which case the key is implicitly concealed in the architecture of the circuit. However, this method has the drawback of more complex manufacture. Besides the reference data possibly stored in the arrangement, the explicitly stored key is the only person-specific parameter in an otherwise universal arrangement.

Besides symmetrical keys, which are fundamentally also suitable for use in the context of the invention, asymmetrical key pairs are particularly suitable above all. In this case, the key (K) would be the private key of the authorized person, that is to say the key which needs to be kept secret. By contrast, the public key would be used to decrypt the encrypted input data in a foreign information system wanting to check the identity or authorization of the person.

Suitable input data (ED) are particularly random or pseudo-random character, number or symbol sequences whose correct encryption can easily be checked by the checking external system and which practically cannot be predicted or guessed by an attacker. The cycle period of these symbol sequences should also be sufficiently long, i.e. virtually infinitely long.

Patent claims

1. An arrangement for capturing and evaluating data or signals, in particular for checking the identity or authorization of a person, etc., having the following features:

a) a device (DE) for capturing data (D) or signals (S);

b) a device (DV) for checking the captured data or signals within the arrangement;

c) a device (KE) for encrypting input data (ED) within the arrangement.

2. The arrangement as claimed in claim 1, in which the captured data or signals are checked by comparing these data or signals or feature data (MD) derived therefrom with reference data (RD) stored in a memory arrangement (SE1) within the arrangement.

3. The arrangement as claimed in one of the preceding claims, in which the input data (ED) are encrypted using a key (K) which is stored in a memory device (SE2) within the arrangement.

4. The arrangement as claimed in one of the preceding claims, in which a device (MT) for transmitting the encrypted input data (ED) is provided.

5. A method for checking the identity or authorization of a person, having the following steps:

a) the person inputs a data item, which needs to be kept secret, into an arrangement, or the arrangement detects a person-specific, in particular biometric, feature of a person, using a sensor device;

b) the data item which has been input or the captured sensor data is or are checked within the arrangement;

c) if the result of the check is positive, input data are encrypted within the arrangement.

6. The method as claimed in claim 5, in which the data item which has been input or the captured sensor data is/are checked by comparing these data or feature

data derived therefrom with reference data stored in a memory arrangement within the arrangement.

7. A method as claimed in one of claims 5 or 6, in which the input data (ED) are encrypted using a key (K) which is stored in a memory device (SE2) within the arrangement.

8. The method as claimed in one of claims 5, 6 or 7, in which the key stored within the arrangement is a private key for the authorized person, and in which the encrypted input data are transmitted to a reception device outside the arrangement using a transmission device (MT) and are checked by the reception device or a device connected downstream thereof by decryption using the public key for the authorized person.

Abstract

Arrangement for capturing and evaluating data or signals, and method for checking the identity or authorization of a person

When checking the identity or authorization of a person, secret or person-specific data are protected against attacks by third parties by checking these data within a protected area. If the result of the check is positive, input data supplied from the outside are encrypted using a key stored within the protected area. The encrypted input data are output. The identity or authorization can then be checked by decryption.

Figure 1

09/890913

99 P 1176

1/1

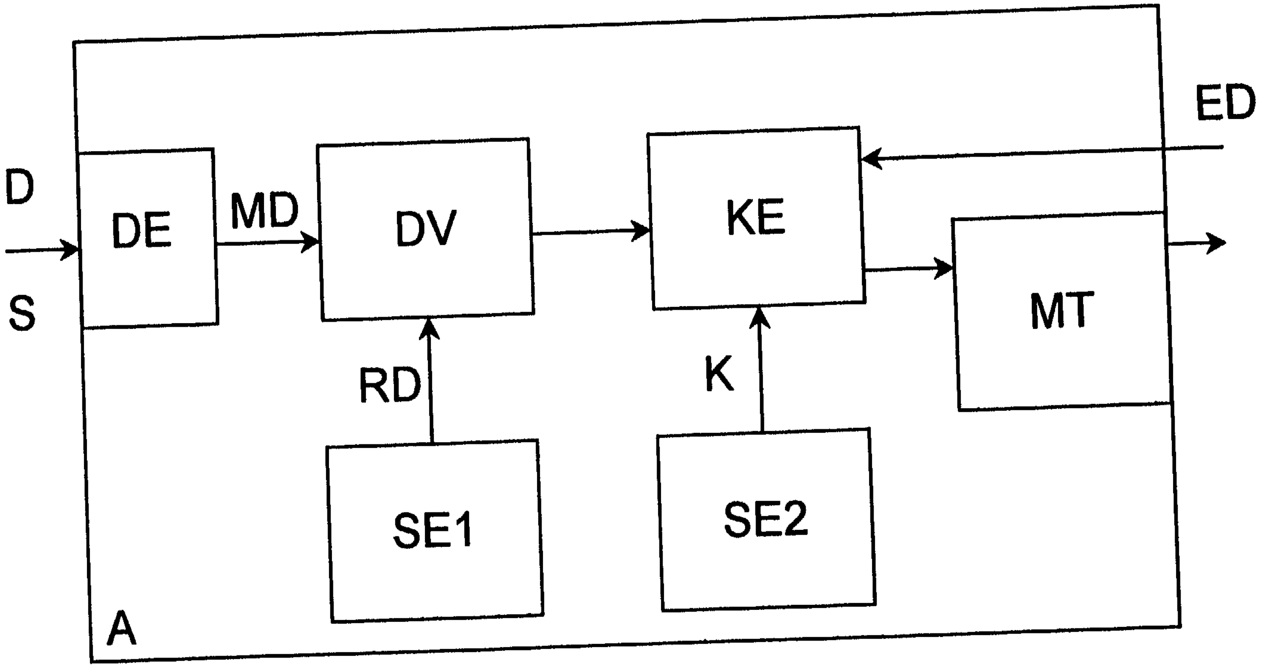

Fig. 1

Declaration and Power of Attorney For Patent Application

Erklärung Für Patentanmeldungen Mit Vollmacht

German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Anordnung zur Erfassung und Auswertung von Daten oder Signalen und Verfahren zur Pruefung der Identitaet oder Berechtigung einer Person

deren Beschreibung

(zutreffendes ankreuzen)
□ hier beigefügt ist.
☒ am 01.02.2000 als
PCT internationale Anmeldung
PCT Anmeldungsnummer PCT/DE00/00284
eingereicht wurde und am _______
abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Arrangement for determining and evaluating data or signals and method for verifying the identity or authorisation of a person

the specification of which

(check one)
□ is attached hereto.
☒ was filed on 01.02.2000 as
PCT international application
PCT Application No. PCT/DE00/00284
and was amended on _______
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

IDNR: 2590 / V: 99-1.00 / B:Val

German Language Declaration

Prior foreign appplications
Priorität beansprucht

			Priority Claimed	
19905033.3 (Number) (Nummer)	DE (Country) (Land)	08.02.1999 (Day Month Year Filed) (Tag Monat Jahr eingereicht)	☒ Yes Ja	□ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	□ Yes Ja	□ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	□ Yes Ja	□ No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

PCT/DE00/00284 (Application Serial No.) (Anmeldeseriennummer)	01.02.2000 (Filing Date D, M, Y) (Anmeldedatum T, M, J)	anhängig (Status) (patentiert, anhängig, aufgegeben)	pending (Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date D,M,Y) (Anmeldedatum T, M; J)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

Customer No. 25227

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

Ext. ______________

Postanschrift:

Send Correspondence to:

Morrison and Foerster LLP
2000 Pennsylvania Ave., NW 20006-1888 Washington, DC
Telephone: (001) 202 887 1500 and Facsimile (001) 202 887 0763
or
Customer No. 25227

Voller Name des einzigen oder ursprünglichen Erfinders: Dr. MANFRED BROMBA 1 - 00	Full name of sole or first inventor: Dr. MANFRED BROMBA
Unterschrift des Erfinders Datum Manfred Bromba 2001-06-26	Inventor's signature Date
Wohnsitz MUENCHEN, DEUTSCHLAND	Residence MUENCHEN, GERMANY DEX
Staatsangehörigkeit DE	Citizenship DE
Postanschrift AM ISARKANAL 24	Post Office Address AM ISARKANAL 24
81379 MUENCHEN	81379 MUENCHEN
Voller Name des zweiten Miterfinders (falls zutreffend):	Full name of second joint inventor, if any:
Unterschrift des Erfinders Datum	Second Inventor's signature Date
Wohnsitz ,	Residence ,
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).